

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-335241

(43)Date of publication of application : 22.11.2002

(51)Int.Cl.

H04L 9/32

G09C 1/00

(21)Application number : 2002-059674

(71)Applicant : HITACHI LTD

(22)Date of filing : 06.03.2002

(72)Inventor : MIYAZAKI KUNIHIKO  
 YOSHIURA YUTAKA  
 SUZAKI SEIICHI  
 SASAKI RYOICHI  
 TAKARAGI KAZUO  
 TOYOSHIMA HISASHI  
 MATSUKI TAKESHI

(30)Priority

Priority number : 2001 816777

Priority date : 22.03.2001

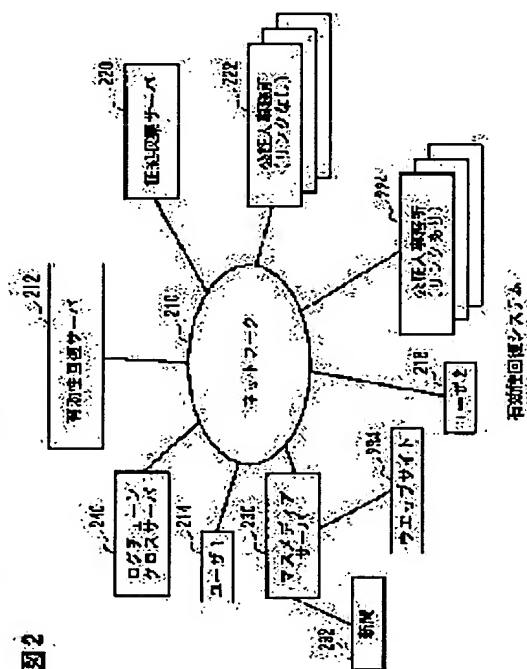
Priority country : US

# (54) METHOD AND SYSTEM FOR RECOVERING VALIDITY OF CRYPTOGRAPHICALLY SIGNED DIGITAL DATA

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide techniques including a method and a system for recovering and/or validating data and/or associated signature log entries.

**SOLUTION:** In the method for validating a restored message having an entry generated in a signature log for a message, where the entry includes cryptographic information associated with the message. When the message is lost, the restored message is generated in response to a request and the restored message is validated by using the signature log. In another embodiment, a method for validating a selected log entry by using a signature log having a plurality of recorded log entries is provided. The method includes a step for computing a cryptographic value for the selected log entry and a step for determining whether the cryptographic value is part of another recorded log entry or not.



## LEGAL STATUS

[Date of request for examination]

07.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-335241

(P2002-335241A)

(43) 公開日 平成14年11月22日 (2002. 11. 22)

(51) IntCl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/32		G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 B

審査請求 未請求 請求項の数40 O L (全 20 頁)

(21) 出願番号 特願2002-59674(P2002-59674)

(22) 出願日 平成14年3月6日(2002. 3. 6)

(31) 優先権主張番号 0 9 / 8 1 6 , 7 7 7

(32) 優先日 平成13年3月22日(2001. 3. 22)

(33) 優先権主張国 米国 (U S)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 宮崎 邦彦

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

(54) 【発明の名称】 暗号化署名付きデジタルデータの有効性を回復する方法とシステム

(57) 【要約】

【課題】 データおよび/または関連する署名ログエントリを復元および/または確認する方法とシステムを含む技術を提供すること。

【解決手段】 メッセージに対して署名ログ中に生成されるエントリを有する復元メッセージを確認する方法が提供される。この時エントリにはメッセージに関連する暗号化情報が含まれる。メッセージが失われている時、復元メッセージが要求に回答して生成され、復元メッセージは署名ログを使用して確認される。他の実施形態では、複数の記録されたログエントリを有する署名ログを使用することによって選択されたログエントリを確認する方法が提供される。この方法には、選択されたログエントリに対する暗号化値を計算するステップと、暗号化値が別の記録されたログエントリの一部であるかを判定するステップとが含まれる。

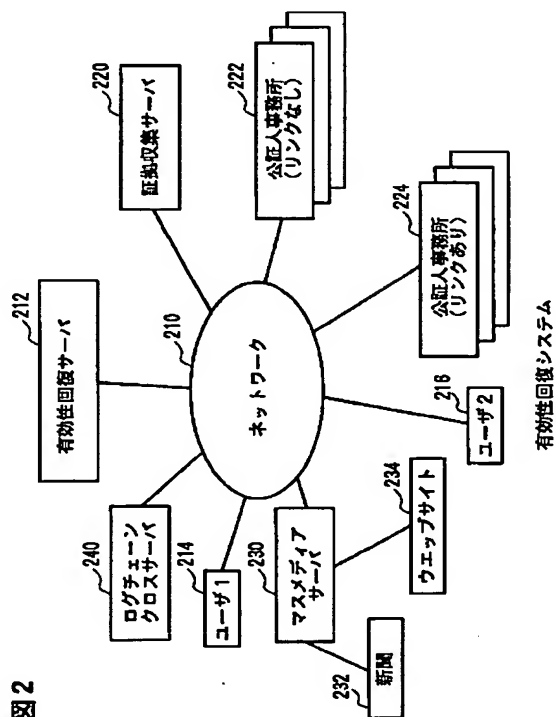


図2

**【特許請求の範囲】**

【請求項1】復元メッセージを確認する方法であって、メッセージに対する署名ログ中のエントリを生成するステップであって、前記エントリが前記メッセージに関連する暗号化情報を含むステップと、前記メッセージが失われている場合、要求に応答して前記復元メッセージを生成するステップと、前記署名ログを使用して前記復元メッセージを確認するステップとを含む方法。

【請求項2】請求項1記載の方法であって、前記署名ログがヒステリシス署名を含む方法。

【請求項3】請求項1記載の方法であって、前記暗号化情報がデジタル署名を含む方法。

【請求項4】請求項3記載の方法であって、前記デジタル署名が前の署名ログエントリからの情報を使用して生成される方法。

【請求項5】ユーザ情報を回復および確認するシステムであって、署名ログを含むユーザシステムであって、前記署名ログが前記ユーザ情報に関連する暗号化情報を含むユーザシステムと、通信ネットワークを介して前記ユーザシステムと結合され、ユーザ情報を復元する回復システムと、前記通信ネットワークを介して前記ユーザシステムと結合され、前記署名ログを使用して復元ユーザ情報を確認する有効性システムとを備えるシステム。

【請求項6】請求項5記載のシステムであって、前記ユーザ情報が前記署名ログのログエントリを含むシステム。

【請求項7】請求項5記載のシステムであって、前記ユーザ情報がユーザメッセージを含むシステム。

【請求項8】請求項5記載のシステムであって、前記暗号化情報がハッシュ値を含むシステム。

【請求項9】請求項5記載のシステムであって、前記署名ログが、前記署名ログの第2のログエントリによって部分的に決定される前記署名ログの第1のログエントリを含むシステム。

【請求項10】ユーザメッセージが有効かどうかを判定するシステムであって、前記システムが、ログを有するユーザコンピュータシステムであって、前記ログが前記ユーザによって送信されるメッセージに関連するログエントリを含み、前記ログエントリが、前記ログの前のログエントリに関連する情報を含むデジタル署名を有するユーザコンピュータシステムと、前記ユーザコンピュータシステムと結合され、前記ログを使用して前記ユーザメッセージを確認する確認ユニットとを備えるシステム。

【請求項11】請求項10記載のシステムであって、さらに、前記ユーザメッセージが失われている時、前記確認ユニットに応答して前記ユーザメッセージを取り出す

収集ユニットを備えるシステム。

【請求項12】請求項10記載のシステムであって、さらに、前記ユーザメッセージが失われている時、前記確認ユニットに応答して前記メッセージの受信機から前記メッセージのコピーを取り出す収集ユニットを備えるシステム。

【請求項13】請求項10記載のシステムであって、さらに、前記ログの選択されたログエントリを公開する公開ユニットを備えるシステム。

【請求項14】請求項13記載のシステムであって、前記選択されたログエントリが前記ユーザメッセージを確認する際使用されるシステム。

【請求項15】請求項13記載のシステムであって、公開ユニットが新聞発行者またはウェブサイトからなるグループから選択されるシステム。

【請求項16】請求項10記載のシステムであって、さらに、前記ログの選択されたログエントリを登録する公証人ユニットを備えるシステム。

【請求項17】請求項10記載のシステムであって、さらに、前記ユーザコンピュータシステムに結合されるログチェーンクロスユニットと、前記ユーザコンピュータシステムと第2のユーザコンピュータシステムの間のトランザクションを記録する前記第2のユーザコンピュータシステムとを備えるシステム。

【請求項18】請求項10記載のシステムであって、さらに、前記ユーザコンピュータシステムに結合されるログチェーンクロスユニットと、前記ユーザコンピュータシステムと第2のユーザコンピュータシステム間のトランザクションを促進する前記第2のユーザコンピュータシステムとを備えるシステム。

【請求項19】メッセージ情報を確認するデータ構造を含むコンピュータ可読データ伝送媒体であって、ユーザメッセージのハッシュを有する第1の部分と、署名ログエントリのハッシュを有する第2の部分と、前記第1の部分と前記第2の部分とに基づくデジタル署名とを含む、コンピュータ可読データ伝送媒体。

【請求項20】請求項19記載のコンピュータ可読データ伝送媒体であって、前記署名ログエントリが前記ユーザメッセージの前の別のユーザメッセージに関連するコンピュータ可読データ伝送媒体。

【請求項21】請求項19記載のコンピュータ可読データ伝送媒体であって、さらにタイムスタンプを有する第3の部分を含むコンピュータ可読データ伝送媒体。

【請求項22】コンピュータを使用して、複数のログエントリを含む署名ログを生成する方法であって、前記方法が、前記複数のログエントリの第1のログエントリを生成するステップであって、前記第1のログエントリが第1のユーザメッセージに関連する第1の暗号化値を含むステップと、

前記複数のログエントリの第2のログエントリを生成するステップであって、前記第2のログエントリが、前記第1のログエントリに関連する第2の暗号化値と、第2のユーザメッセージに関連する第3の暗号化値と、デジタル署名とを含むステップとを含む方法。

【請求項23】請求項22記載の方法であって、前記デジタル署名が前記第2の暗号化値と前記第3の暗号化値とを含む情報を使用して形成される方法。

【請求項24】請求項22記載の方法であって、前記第2の暗号化値が前記第1のログエントリのハッシュである方法。

【請求項25】請求項22記載の方法であって、前記第2のログエントリがさらにタイムスタンプを含む方法。

【請求項26】コンピュータ可読媒体中に格納され、複数のユーザメッセージの選択されたユーザメッセージを確認するデータ構造であって、

前記複数のユーザメッセージの第1のユーザメッセージの第2のハッシュを含む第1のログエントリの第1のハッシュと、

前記複数のユーザメッセージの前記選択されたユーザメッセージの第3のハッシュと、

前記第3のハッシュと結合された前記第1のハッシュのデジタル署名とを含むデータ構造。

【請求項27】コンピュータシステムにおいて、複数の記録されたログエントリを有する署名ログを使用することによって選択されたログエントリを確認する方法であって、前記方法が、

前記選択されたログエントリに対する暗号化値を計算するステップと、

前記暗号化値が前記複数の記録されたログエントリの第1の記録されたログエントリの一部であるかどうかを判定するステップとを含む方法。

【請求項28】請求項27記載の方法であって、前記選択されたログエントリが、前記第1の記録されたログエントリの1つ前の前記複数の記録されたログエントリの第2の記録されたログエントリに対応する方法。

【請求項29】複数のユーザコンピュータシステムの1つによるトランザクションの拒否を防止するシステムであって、前記システムが、

前記複数のユーザコンピュータシステムの第1のユーザと、

前記第1のユーザと前記トランザクションを行う前記複数のユーザコンピュータシステムの第2のユーザと、

前記第1のまたは前記第2のユーザの何れかによる要求に回答して前記トランザクションを記録するログチェーンクロスコンピュータであって、前記記録が前記トランザクションのヒストリシス署名を含むログチェーンクロスコンピュータとを備えるシステム。

【請求項30】コンピュータシステムを使用して、公式に承認された主体によってユーザのログエントリを登録

する方法であって、

前記公式に承認された主体によって署名ログチェーンを維持するステップであって、前記署名ログチェーンの第1のログエントリが前記署名ログチェーンの前の第2のログエントリに関連するステップと、

前記ユーザからユーザログエントリを受信するステップと、

前記ユーザログエントリに関連する暗号化値を生成するステップと、

前記署名ログチェーンの第3のログエントリを生成するステップであって、前記第3のログエントリが前記暗号化値を含むステップとを含む方法。

【請求項31】請求項30記載の方法であって、前記署名ログチェーンの選択されたログエントリが公開される方法。

【請求項32】請求項30記載の方法であって、前記公式に承認された主体が公証人である方法。

【請求項33】ユーザの署名ログを使用するコンピュータシステムによってユーザデータ項目を確認する方法であって、

前記ユーザの署名ログを受信するステップと、

前記ユーザデータ項目に関連する暗号化値が前記ユーザの署名ログ中の第1のログエントリにあるかを確認するステップと、

チェックポイントされた前記ユーザの署名ログ中の第2のログエントリを判定するステップと、

前記第2のログエントリから前記第1のログエントリへの後方連鎖によって前記第1のログエントリを検証するステップと、

結果を前記ユーザに戻すステップとを含む方法。

【請求項34】コンピュータシステムを使用して、2つの時点間のデータ項目を回復する方法であって、

ユーザから2つの時点間のデータを回復せよという要求を受信するステップであって、前記データ項目が前記2つの時点間にあるステップと、

データ回復ユニットから前記データ項目と関連する署名ログエントリとを受信するステップと、

前記関連する署名ログエントリを使用して前記データ項目を確認するステップと、

前記データ項目が確認されたならば、前記データ項目を前記ユーザに送信するステップとを含む方法。

【請求項35】ユーザメッセージを確認するシステムであって、

ユーザから署名ログを受信する入力モジュールであって、前記署名ログが複数の関連ログエントリを含む入力モジュールと、

前記ユーザメッセージから暗号化値を生成する暗号化モジュールと、

前記暗号化値が前記署名ログ中にあることを確認する検証モジュールとを備えるシステム。

【請求項 36】請求項 35 記載のシステムであって、さらに、前記複数の関連ログエントリの第 1 のログエントリが損傷しているかどうかを判定するログ検証モジュールを備え、前記判定が、前記第 1 のログエントリの次の前記複数の関連ログエントリの第 2 のログエントリを選択するステップと、ハッシュ値を示すため前記第 1 のログエントリをハッシュするステップと、前記ハッシュ値が前記第 2 のログエントリの一部であることを確認するステップとを含むシステム。

【請求項 37】復元メッセージを確認するコンピュータプログラム製品であって、メッセージに対して署名ログ中にエントリを生成するコードであって、前記エントリが前記メッセージに関連する暗号化情報を含むコードと、前記メッセージが失われている時、要求に回答して前記復元メッセージを生成するコードと、前記署名ログを使用して前記復元メッセージを確認するコードと、前記コードを具現するコンピュータ使用可能媒体とを含むコンピュータプログラム製品。

【請求項 38】請求項 37 記載のコンピュータプログラム製品であって、前記コンピュータ使用可能媒体が記憶媒体であるコンピュータプログラム製品。

【請求項 39】請求項 37 記載のコンピュータプログラム製品であって、前記コンピュータ使用可能媒体が搬送波であるコンピュータプログラム製品。

【請求項 40】搬送波中に具現される、復元メッセージを確認するコンピュータデータ信号であって、メッセージに対して署名ログ中にエントリを生成するプログラムコードであって、前記エントリが前記メッセージに関連する暗号化情報を含むプログラムコードと、前記メッセージが失われている時、要求に回答して前記復元メッセージを生成するプログラムコードと、前記署名ログを使用して前記復元メッセージを確認するプログラムコードとを含むコンピュータデータ信号。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は一般にデータの回復に関し、特にデジタル署名付きデータの回復および／または確認に関する。

【0002】

【従来の技術】業務および個人両方の通信のためのインターネットの使用は、過去数年間、特に電子商取引の分野で劇的に成長した。ハードウェアおよびソフトウェアの複雑さの増大を伴うこのメッセージトラフィックの大幅な増加によって、データを失う可能性も増大した。コンピュータクラッシュの数が増加しているため、現在多くのシステムはバックアップを提供している。

【0003】従来のデータ回復方法が多数存在するが、

ユーザにとって、回復された情報が不正に変更されているかどうかをどうやって知るかという問題が発生している。これは特にコンピュータのいくつかの広く公表されたアカウントの侵入があった時に言えることである。メッセージ、特に回復されたメッセージへの不正変更があったかを検出する従来の技術の 1 つはデジタル署名である。米国政府はデジタル署名の標準を確立しているが、これは、その全体を引用によって本出願の記載に援用する、連邦情報処理標準公告 (FIPS PUB) 186 に示されている。

【0004】図 1 は、従来のデジタル署名技術を例示する。メッセージ (M) 110 の送信機は署名生成ユニット 112 を有する。メッセージ 110 の受信機は署名検証ユニット 114 を有する。署名生成ユニット 112 はメッセージ 110 を受け取り M110 に対してセキュアハッシュ 116 を行って H (M) 118 を生じる。H

(M) 118 と秘密鍵 120 はデジタル署名アルゴリズム (DSA) 署名 122 に入力され H (M) 118 に対するデジタル署名、すなわち Sign (H (M)) 124 を生じる。M110 と Sign (H (M)) 124 はユーザ送信機の署名生成ユニット 112 からユーザ受信機の署名検証ユニット 114 に送信される。次に M110 は署名検証ユニット 114 でハッシュ 130 され H

(M) 132 を生じる。セキュアハッシュ 130 はセキュアハッシュ 116 と同じ関数である。H (M) 132 と Sign (H (M)) 124 は公開鍵 134 と共に DSA 検証 136 に入力されメッセージ内容が確認される。“no” 結果はメッセージ 110 が不正変更されていることを示し、“yes” 結果は不正変更がないことを示すが、それを保証するわけではない。さらに、デジタル署名はメッセージを認証する、すなわち、メッセージが、そのメッセージが要求された出所からのものであることを受信者に保証する。

【0005】

【発明が解決しようとする課題】しかし、デジタル署名は、解読することが非常に困難であるが不可能ではないと想定される周知のアルゴリズムに依存している。解読困難という想定は、コンピュータの能力の急速な増大と共に次第に説得力がないものになりつつある。さらに、デジタル署名は秘密鍵が秘密のものであることを前提としている。秘密鍵が危殆に瀕した場合、セキュリティはその場で、回復されたデータと共に失われる。従って、回復されたデータを確認するよりよい技術が必要である。

【0006】

【課題を解決するための手段】本発明によれば、データおよび／または関連する署名ログエントリを復元および／または確認する方法とシステムを含む技術が提供される。1 つの態様では、データにはデジタル署名付きユーザメッセージが含まれ、関連署名ログエントリが関連付

け、たとえばリンクされる。各署名ログエントリは、最初のを除いて、前の署名ログエントリからのデータを使用する。前の署名ログエントリからのデータは、現在の署名ログエントリのデジタル署名を形成する際1つの入力として使用される。すなわち、連鎖またはヒステリシス署名が生成される。この態様では、失われたメッセージが復元された後、署名ログが使用され、メッセージに関連するデジタル署名を対応する署名ログエントリと比較することによってメッセージを確認する。署名ログのセキュリティは、公開印刷刊行物、たとえば新聞、ニューズレター、ウェブサイト、雑誌、または定期刊行物といった公開媒体で選択されたエントリを公開することによって向上しうる。メッセージはさらに、公開エントリからメッセージの署名ログエントリに戻る形で署名ログの一貫性を検査することによって確認される。

【0007】本発明の態様の中にはメッセージ用ヒステリシス署名の使用を示すものもあるが、本発明はメッセージに制限されない。たとえば、業務用コンピュータシステム上の一連の業務文書の有効性について、バックアップ媒体からデータを復元した後で、業務用署名ログと各文書に関連するヒステリシス署名を使用してデータを確認することがある。また、ユーザは、ユーザ自身のコンピュータシステム上で、復元されたバックアップデータ、たとえば前の電子商取引購入の確認をしようとすることもある。

【0008】本発明の1つの態様では、メッセージに対して署名ログ中に生成されるエントリを有する復元メッセージを確認する方法を提供されるが、ここでエントリには、メッセージに関連する暗号化情報、たとえばデジタル署名が含まれる。次に、上記メッセージが失われた場合、要求に応答して復元メッセージが生成され、復元メッセージは署名ログを使用して確認される。

【0009】本発明の第2の態様では、ユーザ情報を回復および確認するシステムが提供される。このシステムには、ユーザ情報に関連する暗号化情報を有する署名ログを有するユーザシステムと、通信ネットワークを介してユーザシステムと結合されユーザ情報を復元する回復システムと、上記通信ネットワークを介してユーザシステムと結合され署名ログを使用して復元ユーザ情報を確認する確認システムとが含まれる。

【0010】本発明の第3の態様では、ユーザメッセージが有効かを判定するシステムが提供されるが、このシステムには、ログを有するユーザコンピュータシステムであって、ログがユーザによって送信されたメッセージに関連するログエントリを有し、ログエントリがログの前のログエントリに関連する情報を有するデジタル署名を有するユーザコンピュータシステムと、ユーザコンピュータシステムに結合されログを使用してユーザメッセージを確認する確認ユニットとが含まれる。

【0011】本発明の第4の態様では、メッセージ情報

を確認するデータ構造を含むコンピュータ可読データ伝送媒体が提供される。このデータ構造には、ユーザメッセージのハッシュまたはユーザメッセージ自体を有する第1の部分と、署名ログエントリのハッシュを有する第2の部分と、第1の部分と第2の部分とに基づくデジタル署名とが含まれる。

【0012】本発明の第5の態様では、コンピュータを使用して、複数のログエントリを有する署名ログを生成する方法が提供される。まず、第1のログエントリが生成される。第1のログエントリは第1のユーザメッセージに関連する第1の暗号化値を有する。次に、第2のログエントリが生成される。第2のログエントリは、第1のログエントリに関連する第2の暗号化値と、第2のユーザメッセージに関連する第3の暗号化値と、デジタル署名とを有する。

【0013】本発明の第6の態様では、コンピュータシステムにおいて、複数の記録されたログエントリを有する署名ログを使用することで選択されたログエントリを確認する方法が提供される。この方法には、選択されたログエントリに対する暗号化値を計算するステップと、その暗号化値が別の記録されたログエントリの一部であるかを判定するステップとが含まれる。

【0014】本発明の第7の態様では、複数のユーザコンピュータシステムの1つによるトランザクションの拒否を防止するシステムが提供される。このシステムには、第1のユーザコンピュータシステムと、第1のユーザとトランザクションを行う第2ユーザコンピュータシステムと、第1のまたは第2の何れかのユーザの要求に応答してトランザクションを記録する、ログチェーンクロスコンピュータとが含まれ、この記録にはトランザクションのヒステリシス署名が含まれる。

【0015】本発明の第8の態様では、コンピュータシステムを使用して、公式に承認された主体、たとえば（リンクを有するかまたは有さない）公証人によってユーザのログエントリを登録する方法が提供される。この方法には、公式に承認された主体による署名ログチェーンを維持するステップであって、その際署名ログチェーンの第1のログエントリが署名ログチェーンの前の第2のログエントリに関連するステップと、ユーザからユーザログエントリを受信するステップと、ユーザログエントリに関連する暗号化値を生成するステップと、署名ログチェーンの第3のログエントリを生成するステップであって、その際第3のログエントリが暗号化値を含むステップとが含まれる。

【0016】本発明の第9の態様では、ユーザの署名ログを使用するコンピュータシステムによってユーザデータ項目を確認する方法が提供される。コンピュータシステムはユーザの署名ログを受信し、ユーザデータ項目に関連する暗号化値がユーザの署名ログ中の第1のログエントリにあるかを確認する。次に、コンピュータは、チ

チェックポイントされたユーザの署名ログ中の第2の署名ログを判定した後第2のログエントリから第1のログエントリに後方連鎖することで第1のログエントリを検証し、結果はユーザに戻される。

【0017】本発明の第10の態様では、コンピュータシステムを使用して、2つの時点間のデータ項目を回復する方法が提供される。この方法には、ユーザから2つの時点間のデータを回復せよという要求を受信するステップと、データ回復ユニットからデータ項目と関連署名ログエントリを受信するステップと、関連署名ログエントリを使用してデータ項目を確認するステップと、データ項目が確認された場合、データ項目をユーザに送信するステップとが含まれる。

【0018】本発明の第11の態様では、ユーザメッセージを確認するシステムが提供される。このシステムには、ユーザから複数の関連ログエントリを含む署名ログを受信する入力モジュールと、ユーザメッセージから暗号化値を生成する暗号化モジュールと、暗号化値が署名ログ中にあることを確認する検証モジュールとが含まれる。

【0019】第12の態様では、復元メッセージを確認するコンピュータプログラム製品が提供されるが、これは、メッセージについて署名ログ中に、メッセージに関連する暗号化情報を含むエントリを生成するコードと、メッセージが失われている場合、要求に応答して復元メッセージを生成するコードと、署名ログを使用して復元メッセージを確認するコードと、上記のコードを具現するコンピュータ使用可能媒体とを有する。

【0020】他の態様では、復元メッセージを確認する、搬送波中に具現されるコンピュータデータ信号が提供されるが、これは、メッセージについて署名ログ中に、メッセージに関連する暗号化情報を含むエントリを生成するプログラムコードと、上記メッセージが失われている場合、要求に応答して復元メッセージを生成するプログラムコードと、署名ログを使用して復元メッセージを確認するプログラムコードとを有する。

【0021】本発明のこれらと他の態様は以下の本文および添付の図面に関連してさらに詳細に説明される。

【0022】

【発明の実施の形態】図2は、本発明の有効性回復システムの実施形態を示す。このシステムには、ネットワーク210を介して互いに結合された有効性回復サーバ212とユーザ\_\_1 214とが含まれる。必要に応じて、ユーザ\_\_2 216、証拠収集サーバ220、リンクのない公証人事務所222、リンクのある公証人事務所224、マスメディアサーバ230、マスメディアサーバ230、およびログチェーンクロスサーバ240の1つかそれ以上が含まれ、ネットワーク210を介して互いに結合されることがある。ユーザ\_\_1 214とユーザ\_\_2 216はありうるユーザの例に過ぎず、他の

実施形態には2人より多いユーザが含まれる。マスメディアサーバ230には新聞232および/またはウェブサイト234が含まれる。

【0023】有効性回復サーバ212は証拠収集サーバ220から回復されたメッセージおよび/または署名ログエントリを受信し、メッセージおよび/またはメッセージに関連する署名ログエントリを確認する。ユーザまたは証拠収集サーバ220はマスメディアサーバ230を介して選択された署名ログエントリを公開することを要求することがあり、リンクのない公証人事務所222、またはリンクのある公証人事務所224によって他の選択された署名ログエントリを登録する。この登録または公開によって、署名ログエントリはチェックポイントされ、後で前の署名ログエントリを個々に確認する際使用される。

【0024】証拠収集サーバ220はネットワーク210上で送信されたユーザメッセージに関連する情報を収集しデータベース(DB)中に格納する。この情報には、メッセージに関連する署名ログエントリとそのメッセージの送信相手先が含まれる。この実施形態では、証拠収集サーバ220はそのDB中に全てのユーザの署名ログエントリのコピーを維持しているので、ユーザの署名ログのバックアップの役目を果たしている。メッセージを回復するため、証拠収集サーバ220は誰がメッセージを受信したかを知っており、受信者からメッセージを回復しようとする。代替実施形態では、証拠収集サーバ220はユーザによって送信されたメッセージの一部または全てのコピーを維持し、要求に応じて有効性回復サーバ212にバックアップコピーを供給する。他の実施形態では、証拠収集サーバ220には検索エンジンが含まれるが、これは有効性回復サーバ212の要求に応じて、ネットワーク210を介して失われたメッセージのバックアップコピーを検索する。検索エンジンがバックアップコピーを発見すると、証拠収集サーバはバックアップコピーを取り出し、それを有効性回復サーバ212に転送する。

【0025】公証人事務所222および224は有資格公設または私設の公証人サービスまたは何らかの公式に承認された主体であり、ヒステリシス署名(すなわち、リンクあり)かまたは従来のログブック(すなわち、リンクなし)の何れかを使用して署名ログを維持する。すなわち、ユーザは、公証人サービスによって自分の署名ログに選択されたエントリを定期的に登録できる。こうしたチェックポイントが使用され、個々の前の署名ログエントリを確認する。

【0026】ここで使用されるようなヒステリシス署名は、メッセージに関連する第1の暗号化情報と、少なくとも1つの前のヒステリシス署名に関連する第2の暗号化情報とを含むデジタルデータを使用するセキュリティ機構である。第1の暗号化情報の例はメッセージ暗号化



の結果である。第1の暗号化情報の別の例には、一部または全体がメッセージから形成されたデジタル署名が含まれる。第2の暗号化情報の例には少なくとも1つの前のヒステリシス署名のデジタルデータの暗号化の結果が含まれるが、ここで当初第1のヒステリシス署名は所定の値であることがある。上記の定義を使用すると、ヒステリシス署名の1つの例には、ログエントリのチェーンにおいて、各ログエントリが、最初のログエントリを除いて、前のログエントリに依存する、ログエントリのチェーン中の1つのログエントリが含まれる。

【0027】マスメディアサーバ230は、ユーザまたは証拠収集サーバ220の何れかの要求に応じて、広範な対象者に選択されたユーザ署名ログエントリを公開する。署名ログエントリを公開することで、それが公開された後ログエントリを不正変更することは困難になる。ログエントリを公証人によって登録することと同様、署名ログエントリの公開はエントリをチェックポイントし、特定の前の署名ログエントリを確認するために使用される。新聞発行者232とウェブサイト234という、公開者の2つの例が示される。公開者の他の例には、雑誌、書籍、定期刊行物、ニューズレター、または会議議事録の発行者が含まれる。

【0028】ログチェーンクロスサーバ240は、相互トランザクション、たとえば、連絡、商品の販売、融資、または電子商取引トランザクションが行われる時、たとえば、ユーザ<sub>1</sub> 214とユーザ<sub>2</sub> 216によって使用される。ログチェーンクロスサーバ240は、ヒステリシス署名を使用して署名ログ中にメッセージ転送のコピーを維持する。トランザクション上の紛争が生じた場合、ログチェーンクロスサーバ240はトランザクションの証人の役目を果たす。これによって何れかの当事者がトランザクションを拒否するのが防止される。代替実施形態では、ログチェーンクロスサーバ240はユーザ<sub>1</sub> 214とユーザ<sub>2</sub> 216の間のトランザクションの転送またはメッセージの交換を促進するが、コピーは維持しない。この場合、自分のコピーを維持するのは各ユーザの責任である。

【0029】図3は、図2に示される各コンピュータシステムの1つの実施形態を表すコンピュータシステム310の例を示す。こうした図2のコンピュータシステムには、有効性回復サーバ212、ユーザ<sub>1</sub> 214、ユーザ<sub>2</sub> 216、証拠収集サーバ220、リンクのない公証人事務所222、リンクのある公証人事務所224、マスメディアサーバ230、およびログチェーンクロスサーバ240が含まれる。コンピュータシステム310には、中央処理装置(CPU)312、一時記憶用揮発性記憶装置314(たとえばRAM)、たとえばハードディスク、CD-ROM、またはフレキシブルディスクといった、データおよびソフトウェアを格納する不揮発性記憶装置316、ネットワークに接続するネッ

トワークインターフェース318、ディスプレイ、マウスおよびキーボードに接続するI/Oインターフェース320、および上記の構成要素を互いに接続するバス325が含まれる。別のハードウェア実施形態には、RAIDディスク駆動装置を備えたサーバ用の多重プロセッサMicrosoft Windows NTシステムと、ユーザ用のMicrosoft Windowsオペレーティングシステムを備えたパーソナルコンピュータとが含まれる(Microsoft、Windows、Windows NTは米国Microsoft Corporationの米国およびその他の国における登録商標である)。

【0030】図4は、本発明の1つの実施形態のメッセージ形式410を示す。メッセージは、ネットワーク210上で、ユーザ、たとえばユーザ<sub>1</sub> 214から別のユーザ、たとえばユーザ<sub>2</sub> 216に送信される。メッセージ形式410には、索引番号“i”412と、出所、たとえばユーザ<sub>1</sub> 214のユーザアドレス414が含まれる。さらに、宛先、たとえばユーザ<sub>2</sub> 216のアドレス(図示せず)も含まれる。メッセージ内容、 $M_i$ 、メッセージ内容のハッシュ、 $H(M_i)$ 418、前の $(i-1)$ ログエントリのハッシュ、 $H(P_{i-1})$ 、 $H(P_{i-1})$ と $H(M_i)$ の連結のデジタル署名、すなわち $Sign_i(H(P_{i-1}) || H(M_i))$ 422、および公開鍵証明424が含まれる。メッセージ内容、 $M_i$ にはたとえば、テキスト、HTML、XML、イメージ、ビデオクリップ、音声クリップ、デジタルデータ、またはプログラムが含まれる。1つの実施形態では、メッセージ内容( $M_i$ )には添付ファイルが含まれる。代替実施形態では、添付ファイルは除外される。デジタル署名、 $Sign_i(H(P_{i-1}) || H(M_i))$ 422は、前のログエントリ、 $P_{i-1}$ からの情報がデジタル署名中に含まれているという点でヒステリシス署名である。

【0031】図5は、本発明の他の実施形態の別のメッセージ形式510を示す。メッセージの形式は図4と同様であるが、タイムスタンプ<sub>i</sub>フィールド524が加わっている点が異なっている。1つの実施形態では、タイムスタンプ<sub>i</sub>フィールド524はメッセージが送信された時間である。他の実施形態では、タイムスタンプ<sub>i</sub>フィールド524は、メッセージが作成された時間またはメッセージが受信された時間のこともある。

【0032】図6は、本発明の実施形態のユーザの署名ログの例を示す。各ユーザは時間順で、送信および受信されたメッセージの署名ログを維持する。署名ログエントリは記号 $P_i$ 、たとえば、 $P_1$  610、 $P_2$  620、 $P_{n-1}$  630および $P_n$  640によって表される。最初の署名ログエントリ $P_1$  610はフィールド“IV”612を有するが、これは所定の値に設定された定数である。次のフィールド $H(M_1)$  614は最初のメッセージ内容、 $M_1$ のハッシュである。そして第3のフィールド $Sign_1(IV || H(M_1))$  61

8は、 $H(M_1)$ と連結されたIVのデジタル署名である。次の署名ログエントリ $P_2$  620はフィールド $H(P_1)$  622を有するが、これは前の署名ログエントリ $P_1$  610のハッシュである。次のフィールド $H(M_2)$  624は第2のメッセージ内容、 $M_2$ のハッシュである。第3のフィールド $Sign_2(H(P_1) || H(M_2))$  626は、 $H(M_2)$ と連結された $H(P_1)$ のデジタル署名である。 $n$ 番目の署名ログエントリは $P_n$  640であるが、これには $H(P_{n-1})$  642中に前の署名ログエントリ $P_{n-1}$  630からの情報が含まれる。 $n$ 番目のメッセージ内容、 $M_n$ はハッシュされ、 $H(M_n)$  644を生じる。このデジタル署名はヒステリシス署名、 $Sign_n(H(P_{n-1}) || H(M_n))$  646である。すなわち、 $P_n$ は $[H(P_{n-1}) || H(M_n) || Sign_n(H(P_{n-1}) || H(M_n))]$ に等しい。 $(n-1)$ 番目の署名ログエントリは $P_{n-1}$  630であるが、これには $H(P_{n-2})$  632中に前の署名ログエントリ $P_{n-2}$ からの情報が含まれる。 $(n-1)$ 番目のメッセージ内容、 $M_{n-1}$ はハッシュされ、 $H(M_{n-1})$  634を生じる。このデジタル署名はやはりヒステリシス署名、 $Sign_{n-1}(H(P_{n-2}) || H(M_{n-1}))$  636である。すなわち、各ログエントリ、 $P_i$ は、前のログエントリ、 $P_{i-1}$ に向かって後方に連鎖

$$H(P_{j-1})=H[H(P_{j-2})||H(M_{j-1})||Sign_{j-1}(H(P_{j-2})||H(M_{j-1}))]$$

【0036】次に、ステップ814で、計算された $H(P_{j-1})$ が $P_j$ に対するユーザの署名ログ中にあるかを検査する。答えがノーであれば、ステップ818で署名ログは損傷している。答えがイエスであれば、 $j-1$ が $m$ より大きいか検査される(ステップ820)。ノーであれば、処理は完了し822、署名ログエントリ $P_m \sim P_{k-1}$ が確認される( $P_k$ は前に確認されると想定する)。イエスであれば、 $j$ は1つ減らされ、処理はステップ812に進んで $H(P_{j-1})$ を計算する。

【0037】たとえば、 $k=5$ で $m=3$ であるとする。ステップ810では $j=k=5$ である。ステップ812では、 $P_4$ に対する署名ログエントリを使用して $H(P_4)$ が計算される。次に、図6から示されているように、 $P_5$ に対するユーザの署名ログ中に $H(P_4)$ があるかが検査される。答えがイエスであれば、 $P_5$ が前に確認されていると想定すれば $P_4$ は確認される。 $(5-1)>3$ (ステップ820)であるので、 $j$ は1つ減らされる(ステップ824で $j=4$ )。ステップ812で $P_3$ に対するログエントリから $H(P_3)$ が計算され、計算された $H(P_3)$ がログエントリ $P_4$ 中の対応するフィールドに対して検査される。 $H(P_3)$ が署名ログ中にあるならば、 $P_3$ が確認され、ステップ820で、 $(4-1)>3$ が検査される。答えはノーなので、処理

する。この連鎖によって、現在の情報と共に過去の情報も知らなければならないため、デジタル署名を偽造する困難は大きく増大する。他の実施形態では、ユーザは別個の送信ログと受信ログを有することがある。

【0033】図7は、本発明の他の実施形態のユーザ署名ログの例を示す。この署名ログエントリは図6と同様であるが、各エントリの追加タイムスタンプフィールド、たとえば、716、726、736、および746がある点が異なっている。タイムスタンプフィールドは図5のものと同じである。

【0034】図8は、本発明の実施形態の署名ログファイル中のログエントリの確認を示すフロー図を示す。 $k>m$ である2つのログエントリ $P_k$ と $P_m$ がある場合、 $P_m \sim P_{k-1}$ の計算済みハッシュがユーザの署名ログファイル中になければならず、そうでない場合署名ログは損傷している。ステップ810では、 $P_k$ と $P_m$ が、たとえば有効性回復サーバ212によって受信される。 $j>k$ であり、一時反復索引“ $j$ ”は当初 $k$ に設定される。ステップ812では、 $H(P_{j-1})$ が $P_{j-1}$ のハッシュを発見することによって計算される、すなわち次式である。

【0035】

【数1】

はステップ822で終了し、結果として $P_3$ および $P_4$ が確認された。 $P_5$ は、チェックポイントによって、たとえばマスメディアサーバ230を使用して $P_5$ を公開するか、または公証人222および224によって $P_5$ を登録することで前もって確認することができる。チェックポイントの意味は、 $P_5$ がチェックポイントされた後不正変更することが困難になるということである。

【0038】図9は、本発明の1つの実施形態のチェックポイントの例を示す。縦軸840は時間を表し、相対時間 $t=0$  841で始まる。最初の署名ログエントリ842は図6の $P_n$ と同様の形式を有する。次のログエントリは844によって示される。ログエントリ846は時間862( $t=t_1$ )で発生し、この例では第1のチェックポイントを表す。これは、ログエントリ846が公開されるかまたは公証人によって登録されたことを意味する。846が $P_5$ でチェックポイントされ、844が $P_3$ ( $P_4$ は図示せず)であるとする。図8が使用され $P_3$ および $P_4$ を確認することがある。 $t=t_2$  864の時間、すなわち、署名ログ850と852の間にログの損傷があるならば、ログエントリ852、854、および856が疑わしい。時間 $t=t_3$  866でのチェックポイント856は、損傷したログエントリが公開または登録されているため意味がない。ログエントリ848および850はまだ有効である。損傷がメッセ

ージに対するものであって署名ログに対するものでないならば、ログエントリ856（チェックポイント2）から846（チェックポイント1）への後方連鎖を行う時に損傷が検出される見込みがある。従って、ユーザの署名ログを保護することが重要である。

【0039】図10は、本発明の実施形態のログチェーンクロスサーバを使用する例を示す。アリスとボブという2人のユーザがあり、彼らはトランザクション、たとえば商品販売の提案と受け入れを行おうとしているとする。アリスは、ログエントリ912、914、916、および918を含む署名ログ910を有し、ボブは、ログエントリ932、934、936、および938を含む署名ログ930を有する。凡例は、アリスのヒステリシス署名フロー920とボブのヒステリシス署名フロー940を示す。トランザクションは、ボブとアリスの両方がトランザクションを促進するログチェーンクロスサーバ240に接触することによって開始される。ボブはログチェーンクロスサーバ922を介してアリスに自分の提案メッセージを送信する。提案メッセージに関連するログエントリ934がボブの署名ログ930に入力される。ログチェーンクロスサーバ240はボブからの提案を受信すると、対応する署名ログエントリをログに記録し、提案メッセージをアリスに送信する。アリスは、提案メッセージを受信すると、自分の署名ログ910にログエントリ914を記録する。次にアリスはボブの宛先と共に受け入れメッセージをログチェーンクロスサーバ240に送信する。アリスは受け入れメッセージに関連する署名ログエントリ916を自分の署名ログ910に入力する。ログチェーンクロスサーバ240は受け入れメッセージを受信すると、対応する署名ログエントリをログに記録し、メッセージをボブに伝える。ボブは受け入れメッセージを受信すると署名ログエントリ936を自分の署名ログ930に入力し、トランザクションは完了する。すなわち、トランザクション、すなわち提案および受け入れメッセージがログエントリを有する場所は、アリスのログ910、ボブのログ930、およびログチェーンクロスサーバ240のログと3つある。これによってアリスまたはボブが後でトランザクションを拒否することが防止される。ログチェーンクロスサーバ240はトランザクションの公平な証人の役目を果たす。

【0040】図11は、リンクのある公証人による署名ログエントリの登録の例を示す。すなわち、公証人はヒステリシス署名または連鎖ログ1030を有する。ユーザはヒステリシス署名ログ1010を有し、これにはエントリ1012、1014、および1016が含まれる。公証人はヒステリシス署名ログ1030を有し、これにはログエントリ1032、1034、1036、および1038が含まれる。この実施形態では公証人は、マスメディアサーバ230を使用して、そのログエントリ、たとえばエントリ1034およびエントリ1038

を定期的に公開する。ユーザは、ログエントリ、たとえばエントリ1014を公証人に送信することによって登録できる。次に公証人はユーザのログエントリ1014を公証人の署名ログ1030に入力し、エントリ1036に与える。すなわち、ユーザのログエントリは公証人のログチェーンの一部となる。

【0041】図12は、本発明の実施形態のマスメディアサーバ230に関するフロー図を示す。ステップ1110では、マスメディアサーバ230は、ユーザログエントリ $P_i$ を公開せよというユーザ要求を受信する。次にマスメディアサーバ230は公開者、たとえばウェブサイト234または新聞232に、ログエントリ項目 $P_i$ を送信する。公開の後、ステップ1114では、マスメディアサーバ230は公開者からタイムスタンプ、たとえば $P_i$ が公開された日付／時間を受信する。ステップ1116では、 $P_i$ が公開者のIDおよび／または公開の日付／時間と共に格納される。ステップ1118では、マスメディアサーバ230は有効性回復サーバ212に要求ユーザID、公開者、および／または公開の日付／時間を通知する。そしてステップ1120では、ユーザは公開者および／または公開の日付／時間を通知される。

【0042】図13は、本発明の実施形態において署名ログエントリがチェックポイントされているかを判定する有効性サーバを示すフロー図を示す。ステップ1210では、有効性回復サーバ212は $P_i$ がチェックポイントされたかを判定せよという要求を受信する。有効性回復サーバ212は、可能性のある公開者または公証人のユーザによって索引付けされるリストを検索する（ステップ1212）。次に有効性回復サーバ212は、可能性のある公開者または公証人があればその識別情報を含む要求をマスメディアサーバ230または公証人222または224に送信する。この要求は $P_i$ が公開／公証されているかを問い合わせるものである。ステップ1216では、イエスの答えが公開者または公証人の名称および／または日付／時間と共にマスメディアサーバから受信される。答えがノーであれば、「公開されていない」という回答だけが戻される。

【0043】図14は、ユーザ署名ログエントリ、 $P_i$ を確認する有効性回復サーバの実施形態を示す。ステップ1420では、有効性回復サーバ212は署名ログエントリ $P_i$ を確認せよというユーザ要求を受信する。 $P_i$ には $H(M_i)1410$ 、 $H(P_{i-1})1412$ および $Sign_i(H(M_i) || H(P_{i-1}))1414$ が含まれる。有効性回復サーバ212はまず、たとえば図1のDSA検証136を使用することでデジタル署名を検証する（ステップ1422）。DSA検証136への入力には $H(M_i) || H(P_{i-1})$ 、 $Sign_i(H(M_i) || H(P_{i-1}))1414$ 、および公開鍵134である。デジタル署名が検証されるならば

(ステップ1422のイエス結果)、有効性回復サーバ212はユーザからユーザ署名ログを要求し受信する(ステップ1424)。ステップ1426では、 $H(M_i)$ 1410と $H(P_{i-1})$ 1412が、ユーザの署名ログ中の対応する値に対して検査される。こうしたハッシュ値がログ中にあるならば、ステップ1428で、 $k$ が $i$ より大きいとか $i$ に等しい、チェックポイントされた $P_k$ が探索される。図8のフロー図を使用して、ユーザの署名ログの一貫性が、チェックポイント $P_k$ から $P_i$ に戻って検査される(ステップ1430)。署名ログが損傷していないならば、肯定的な確認結果がユーザに送信される(ステップ1432)。

【0044】図15は、ユーザメッセージ内容、 $M_i$ を確認する有効性回復サーバの実施形態を示す。ステップ1520では、有効性回復サーバ212はデータ $M_i$ を確認せよというユーザ要求を受信する。メッセージには $M_i$ 1510、 $H(M_i)$ 1512、 $H(P_{i-1})$ 1514、および $Sign_i(H(M_i) || H(P_{i-1}))$ 1516が含まれる。有効性回復サーバ212はまず、 $M_i$ のハッシュを計算し、それが $H(M_i)$ 1512と同じであるか検査する(ステップ1521)。

第2に、デジタル署名が、たとえば図1のDSA検証136を使用することで確認される(ステップ1522)。DSA検証136への入力は $(H(M_i) || H(P_{i-1}))$ 、 $Sign_i(H(M_i) || H(P_{i-1}))$ 1516、および公開鍵134である。デジタル署名が検証されるならば(ステップ138のイエス結果)、有効性回復サーバ212はユーザからユーザ署名ログを要求し受信する(ステップ1524)。ステップ1526では、 $H(M_i)$ 1512と $H(P_{i-1})$ 1514が、ユーザの署名ログ中の対応する値に対して検査される。こうしたハッシュ値がログ中にあるならば、次にステップ1528で、 $k$ が $i$ より大きいとか $i$ に等しい、チェックポイントされた $P_k$ が探索される。図8のフロー図を使用して、ユーザの署名ログの一貫性が、チェックポイント $P_k$ から $P_i$ に戻って検査される(ステップ1530)。署名ログが損傷していないならば、 $M_i$ に関する肯定的な確認結果がユーザに送信される(ステップ1532)。

【0045】表1は、障害と回復の表を示す。

【0046】

【表1】

表1

損失	原因の例	回復
署名ログエントリ、 $P_i$	記憶媒体の障害	バックアップファイル。 バックアップファイルがない場合、 証拠収集サーバから $P_i$ を取り出して確認する
データ、 $M_i$	記憶媒体の障害、 ユーザの誤り	バックアップファイル。 バックアップファイルがない場合、 証拠収集サーバから $M_i$ および $P_i$ を取り出して 確認する
データセキュリティ (データまたはログエントリは 損失していないが、 データまたはログエントリの 有効性が不明) —ユーザは誠実	秘密鍵の漏洩、 メッセージの不正な 変更または挿入	ユーザの署名ログ および チェックポイント
データセキュリティ —ユーザが不正に変更	ユーザによる ログの変更、 ユーザによる メッセージの拒否	ログチェーンクロス、 および チェックポイント

【0047】各縦列の見出しは、失われる情報の種類、損失の原因の例、および可能性のある回復方法である。署名ログエントリ $P_i$ の損失は、たとえば記憶媒体の障害によって発生する。可能性のある回復方法はバックアップファイルから署名ログエントリを回復することである。バックアップファイルが存在しない場合、 $P_i$ のコピー、すなわち、 $H(M_i)$ 、 $H(P_{i-1})$ 、および

$Sign_i(H(M_i), H(P_{i-1}))$ が証拠収集サーバ220のDBから取り出され、有効性回復サーバ212は、図14に示された手順を使用して署名ログエントリ $P_i$ を確認するよう要求される。

【0048】メッセージ内容 $M_i$ の損失が記憶媒体の障害またはユーザの誤りによって発生している場合、可能性のある回復手順にはバックアップファイルからの復元

が含まれる。バックアップファイルが存在しない場合、証拠収集サーバ220は、メッセージ内容 $M_i$ と、関連する署名ログエントリ $P_i$ を取り出して戻すように要求される。次に、有効性回復サーバ212は、図15に示される手順を使用してメッセージ内容 $M_i$ を確認するように要求される。

【0049】メッセージ内容または署名ログエントリは失われていないがデータ $M_i$ または署名ログエントリ $P_i$ の有効性が不明であるというようなデータセキュリティの損失は、ユーザの秘密鍵の危殆化、メッセージの不正な変更または挿入によって発生する。ユーザすなわちメッセージの作成者が誠実で、ユーザ、たとえばユーザ\_1 214によって維持されるユーザ署名ログが損傷していない場合、可能性のある回復手順には、図14および図15に示された手順を使用し、ユーザ署名ログと関連するチェックポイントを使用して $M_i$ または $P_i$ を確認することが含まれる。

【0050】たとえば、メッセージのユーザ/第3者による変更またはユーザによる拒否による署名ログの損傷に起因するデータセキュリティの損失がある場合、回復は原因に基づく。ユーザがトランザクションメッセージを不正変更および拒否した場合、トランザクションの際に交換されたメッセージのコピーがログチェーンクロスサーバ240を使用して回復される。第3者がユーザの署名ログを変更した場合、損傷以前の最後の公開/登録された署名ログエントリが使用される。この公開/登録された署名ログエントリの前の全てのログエントリは回復および確認することができる。

【0051】図16は、本発明の実施形態においてデータを収集する証拠収集サーバのフロー図を示す。ステップ1710では、証拠収集サーバ220はユーザから証拠メッセージを受信する。証拠メッセージには、 $P_i$ 、 $M_i$ の日付/時間、索引 $I$ 、 $M_i$ の送信機のアドレスまたはID、 $M_i$ の受信機のアドレスまたはID、またはユーザの送信時間の中、1つかそれ以上が含まれる。代替実施形態では、証拠メッセージは図4または図5の何れかに示される形式のものである。ステップ1712では、証拠メッセージはユーザアドレスまたはIDによって索引付けされる証拠収集サーバのデータベース(DB)に格納される。

【0052】図17は、本発明の実施形態においてデータを回復する証拠収集サーバのフロー図を示す。ステップ1810では、証拠収集サーバ220は有効性回復サーバ212からメッセージ内容 $M_i$ を回復せよという要求を受信する。ステップ1812では、証拠収集サーバ220はそのデータベースから $M_i$ に関連する証拠メッセージを検索する。次にステップ1814で、証拠収集サーバ220は、 $M_i$ を受信したユーザから $M_i$ と $P_i$ のコピーを証拠収集サーバに戻すよう要求する。代替実施形態では、証拠収集サーバ220はすでにそのDBに

格納された $M_i$ と $P_i$ のコピーを有しておりこれらのコピーを使用する。また他の実施形態では、証拠収集サーバは $P_i$ を有し、ネットワーク210を検索して $M_i$ を回復する。次に $P_i$ が検査され、受信された $P_i$ が証拠収集サーバのデータベース中の $P_i$ と同じかが調べられる(ステップ1816)。 $P_i$ がDB中にあるならば、ステップ1818で、 $M_i$ と $P_i$ は確認のため有効性回復サーバ212に送信される。

【0053】図18は、他の実施形態においてユーザ署名ログエントリを回復する有効性回復サーバのフロー図を示す。ステップ1910では、ユーザ、たとえばユーザ\_1 214は有効性回復サーバ212に署名ログエントリ $P_i$ を回復せよという要求を行う。ステップ1912では、一時変数“j”はiに等しく設定される。次にステップ1914では、証拠収集サーバ220に対して $P_j$ を入手して戻すようにという要求がなされる。次に有効性回復サーバ212は、図1に示された手順を使用し、 $H(M)$ の代わりに $(H(P_{i-1}) || H(M_i))$ によって $P_j$ のデジタル署名を検証する(ステップ1916)。

【0054】ステップ1918では、 $P_j$ が検査され、チェックポイントされているかが調べられる。答えがイエスであれば、ステップ1920で、図8に示された手順を使用して、ユーザ署名ログの一貫性がチェックポイント $P_j$ から署名ログエントリ $P_i$ に戻って検査される。そしてユーザの署名ログ中の $P_i$ が損傷していないならば、 $P_i$ はステップ1922でユーザに戻される。ステップ1918の答えがノーであれば、 $P_j$ はログエントリの一時順次リストまたは待ち行列に入力され(ステップ1924)、jが1つ増やされて(ステップ1926)ステップ1914~1918が繰り返される。連鎖ログエントリを含むリストをチェックポイントした $P_j$ が発見されると、ステップ1920で $P_j$ から $P_i$ に戻ってログエントリの一貫性を検査するために使用される。

【0055】図19は、他の実施形態においてユーザメッセージを回復する有効性回復サーバのフロー図を示す。ステップ2010では、ユーザ、たとえばユーザ\_1 214は有効性回復サーバ212にメッセージ内容 $M_i$ を回復せよという要求を行う。次にステップ2012では、証拠収集サーバ220に対して $M_i$ および関連する署名ログエントリ $P_i$ を入手して戻すようにとの要求がなされる。ステップ2013では、 $M_i$ のハッシュが $P_i$ 中にあるかが検査される。ステップ2014では、一時変数“j”は“i”に等しく設定される。ステップ2016では、証拠収集サーバ220に対して $P_j$ を入手し戻すようにとの要求がなされる( $i=j$ の時、 $P_i$ はステップ2012で前に入手されているのでこのステップは省略される)。

【0056】次に有効性回復サーバ212は、図1に示

された手順を使用し、H (M) の代わりに (H (P<sub>i-1</sub>) || H (M<sub>i</sub>)) によって P<sub>j</sub> のデジタル署名を検証する (ステップ 2018)。ステップ 2020 では、P<sub>j</sub> が検査され、チェックポイントされているかが調べられる。答えがイエスであれば、ステップ 2022 で、図 8 に示された手順を使用して、ユーザ署名ログの一貫性がチェックポイント P<sub>j</sub> から署名ログエントリ P<sub>i</sub> に戻って検査される。そしてユーザの署名ログ中の P<sub>i</sub> が損傷していないならば、M<sub>i</sub> はステップ 2024 でユーザに戻される。ステップ 2020 の答えがノーであれば、P<sub>j</sub> はログエントリの一時順次リストまたは待ち行列に入力され (ステップ 2026)、j が 1 つ増やされてステップ 2016 ~ 2020 が繰り返される。連鎖ログエントリを含むリストをチェックポイントした P<sub>j</sub> が発見されると、ステップ 2022 で P<sub>j</sub> から P<sub>i</sub> に戻ってログエントリの一貫性を検査するために使用される。

【0057】図 20 は、他の実施形態の 2 つの時点間のユーザメッセージを回復する有効性回復サーバのフロー図を示す。この実施形態では、ユーザメッセージは図 5 の形式であり、タイムスタンプフィールド 524 が存在する。ステップ 2050 では、ユーザは時間 t<sub>1</sub> と時間 t<sub>2</sub> の間のメッセージ M<sub>j</sub> を回復せよという要求を有効性回復サーバ 212 に送信する。有効性回復サーバ 212 は、証拠収集サーバ 220 から M<sub>j</sub> と関連する P<sub>j</sub> を要求する (ステップ 2052)。ステップ 2054 では、有効性回復サーバ 212 は図 15 の手順を使用して M<sub>j</sub> を確認する。ステップ 2056 では、有効性回復サーバ 212 または証拠収集サーバ 220 は、t<sub>1</sub> と t<sub>2</sub> の間に別の M<sub>j</sub> が存在するかを検査する。存在する場合、ステップ 2052 ~ 2056 が繰り返される。答えがノーであれば、M<sub>j</sub> がユーザに送信される。他の実施形態では、M<sub>j</sub> は証拠収集サーバから一括して入手される。すなわちステップ 2052 は t<sub>1</sub> と t<sub>2</sub> の間の全ての M<sub>j</sub> を戻すようにという証拠収集サーバ 220 に対する一括要求となり、ステップ 2054 および 2056 は必要なくなる。

【0058】上記の実施形態は一般に特定のハードウェアおよびソフトウェアに関して説明されたが、認識されるように、本発明はさらに広範な適用可能性を有する。たとえば、ソフトウェア機能はさらに結合され、またさらには分離されることがある。同様に、ハードウェア機能もさらに結合され、またさらには分離されることがある。ソフトウェア機能がハードウェアまたはハードウェアとソフトウェアの組み合わせによって実現されることもある。同様に、ハードウェア機能がソフトウェアまたはハードウェアとソフトウェアの組み合わせによって実現されることもある。適用業務に応じて、任意の数の異なった組み合わせが行われることがある。

【0059】上記の教示を考慮して本発明の多くの修正

および変形が可能である。従って、理解されるように、添付の請求項の範囲内で、本発明は上記で特に説明された以外の形で実施されることがある。

#### 【0060】

【発明の効果】本発明によれば、データおよび/または関連する署名ログエントリを復元および/または確認することが可能になる。

#### 【図面の簡単な説明】

【図 1】従来のデジタル署名技術 (先行技術) を例示する。

【図 2】本発明の有効性回復システムの実施形態を示す。

【図 3】図 2 に示されるコンピュータシステムの 1 つの実施形態を表すコンピュータシステムの例を示す。

【図 4】本発明の 1 つの実施形態のメッセージ形式を示す。

【図 5】本発明の他の実施形態の別のメッセージ形式を示す。

【図 6】本発明の実施形態のユーザの署名ログの例を示す。

【図 7】本発明の他の実施形態のユーザの署名ログの例を示す。

【図 8】本発明の実施形態の署名ログファイル中のログエントリの確認を示すフロー図を示す。

【図 9】本発明の 1 つの実施形態のチェックポイントの例を示す。

【図 10】本発明の実施形態のログチェーンクロスサーバを使用する例を示す。

【図 11】本発明の実施形態のリンクを有する公証人による署名ログの登録の例を示す。

【図 12】本発明の実施形態のマスメディアサーバ 230 に関するフロー図を示す。

【図 13】本発明の実施形態において署名ログエントリがチェックポイントされているかを判定する有効性サーバを示すフロー図を示す。

【図 14】ユーザ署名ログエントリを確認する有効性回復サーバの実施形態を示す。

【図 15】ユーザメッセージ内容を確認する有効性回復サーバの実施形態を示す。

【図 16】本発明の実施形態においてデータを収集する証拠収集サーバのフロー図を示す。

【図 17】本発明の実施形態においてデータを回復する証拠収集サーバのフロー図を示す。

【図 18】本発明の他の実施形態においてユーザ署名ログエントリを回復する有効性回復サーバのフロー図を示す。

【図 19】本発明の他の実施形態においてユーザメッセージを回復する有効性回復サーバのフロー図を示す。

【図 20】本発明の他の実施形態の 2 つの時点間のユーザメッセージを回復する有効性回復サーバのフロー図を

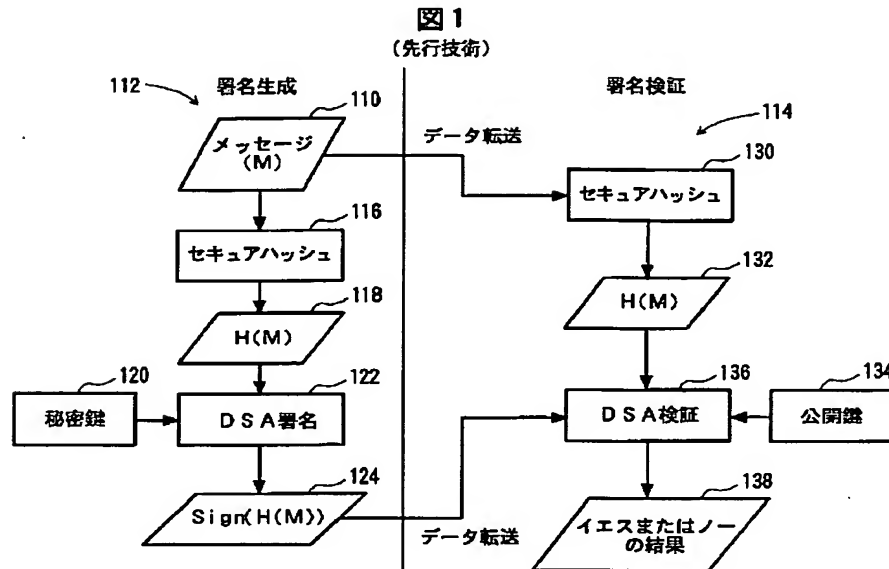
示す。

【符号の説明】

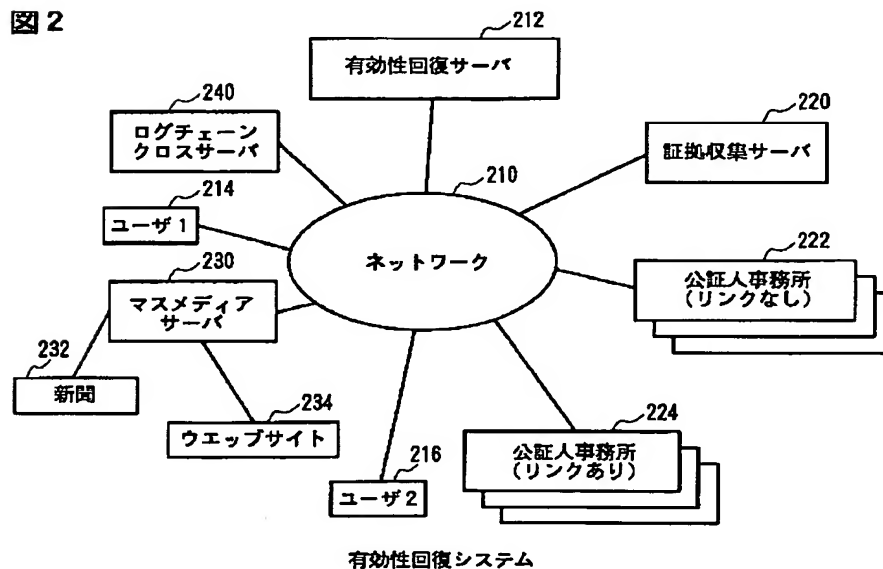
210…ネットワーク、212…有効性回復サーバ、214…ユーザ1、216…ユーザ2、220…証拠収集サーバ

サーバ、222…公証人事務所（リンクなし）、224…公証人事務所（リンクあり）、230…マスメディアサーバ、232…新聞、234…ウェブサイト、240…ログチェーンクロスサーバ

【図1】

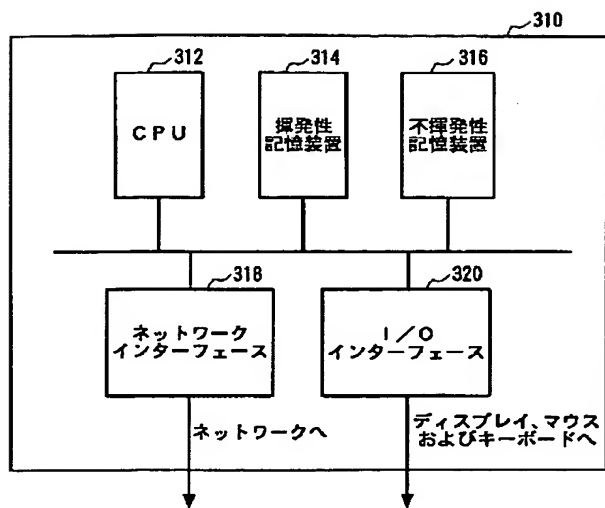


【図2】



【図 3】

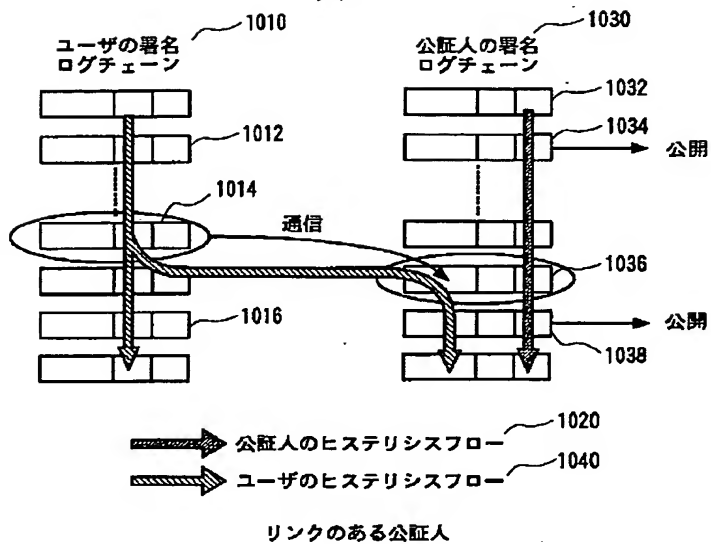
図 3



コンピュータの例

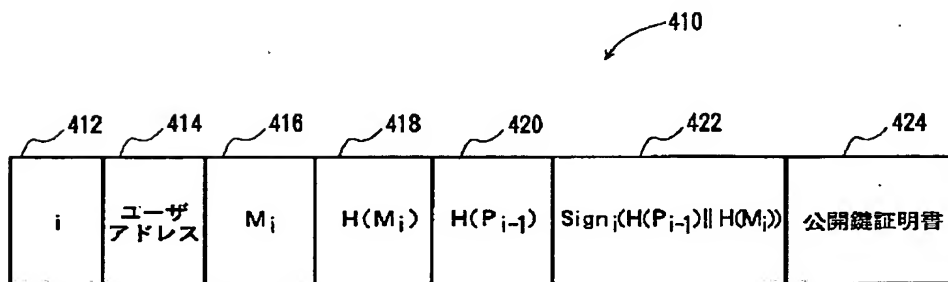
【図 11】

図 11



【図 4】

図 4

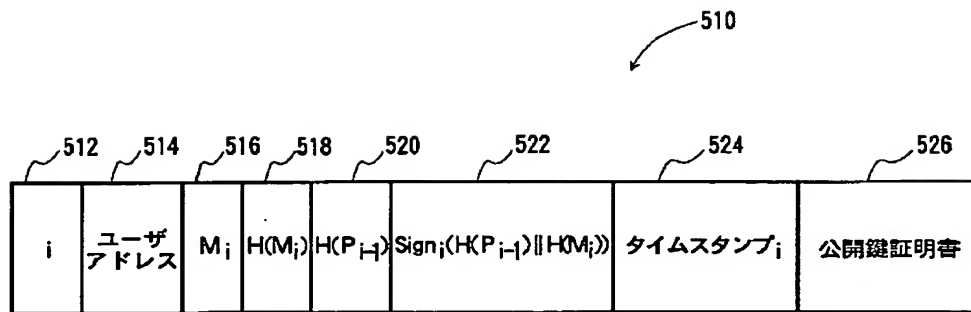


メッセージ形式



【図5】

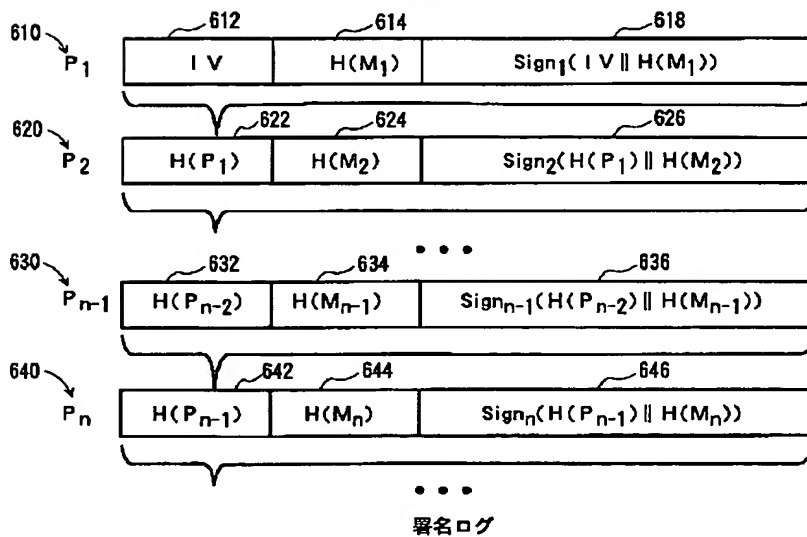
図5



タイムスタンプを伴うメッセージ形式

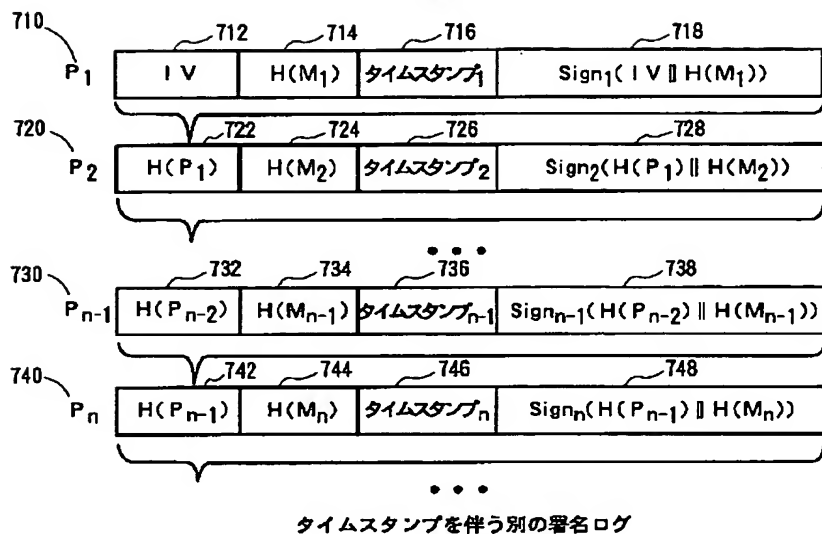
【図6】

図6



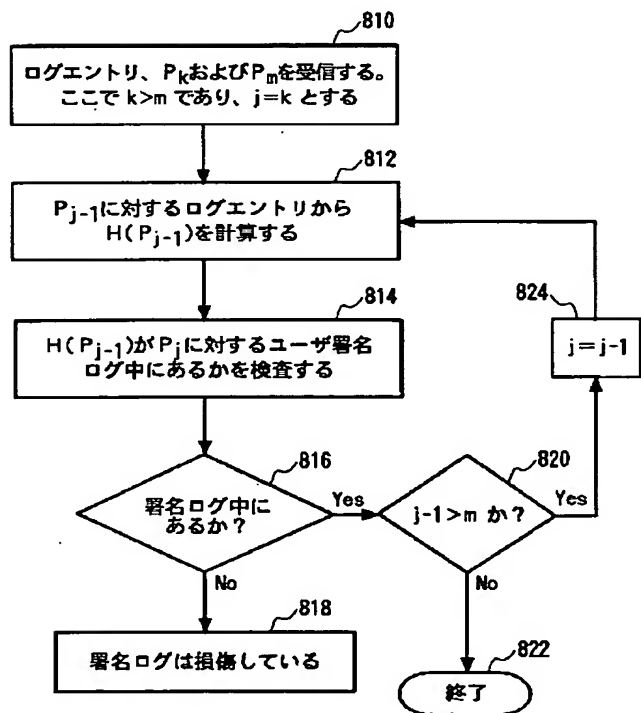
【図7】

図7



【図8】

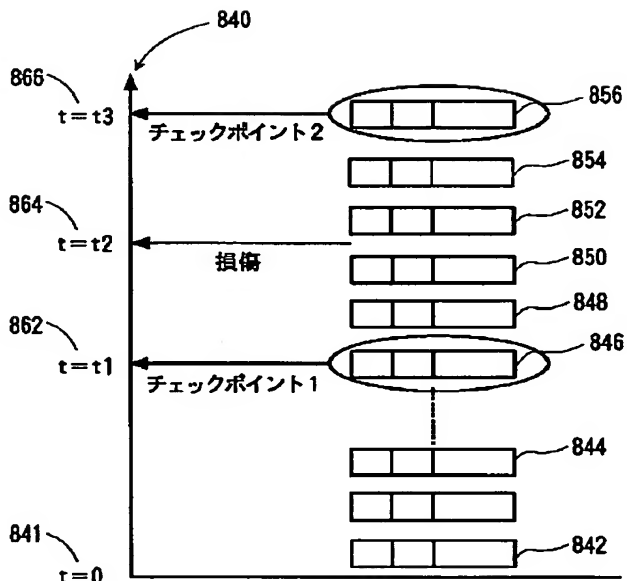
図8



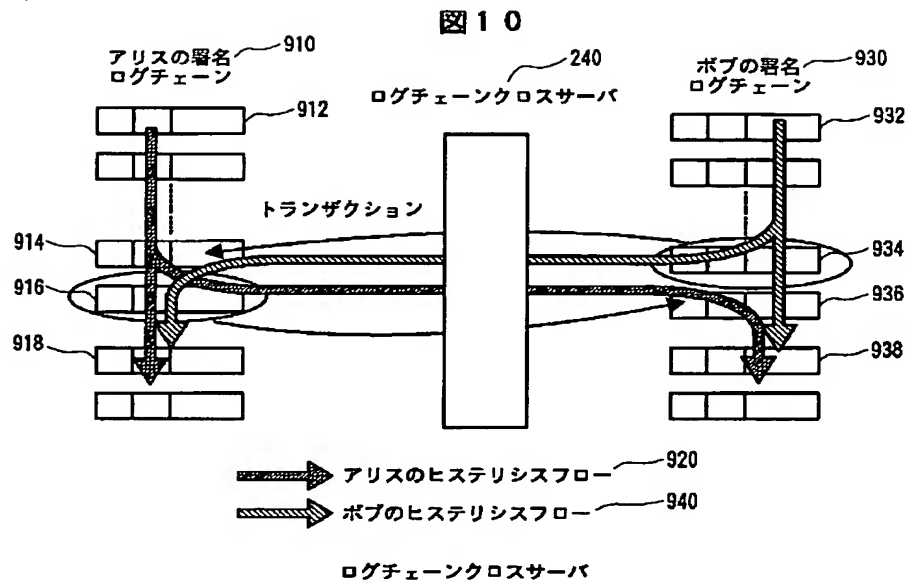
ログエントリの確認一後方連鎖

【図9】

図9

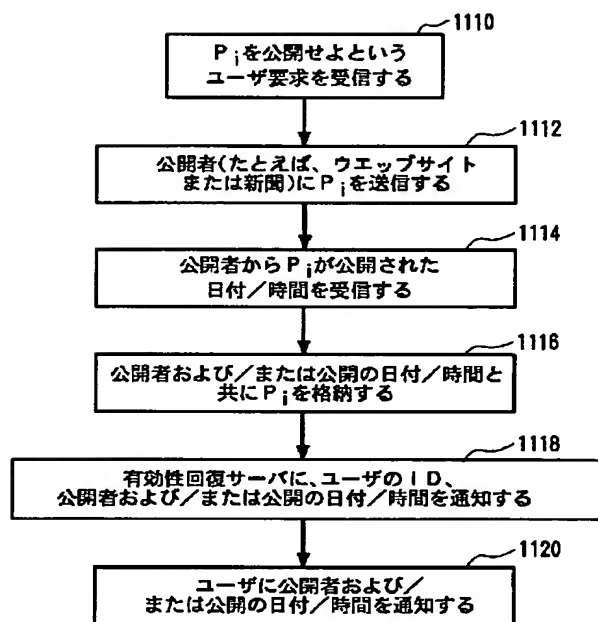
ログエントリのチェックポイント  
(たとえば、公開または公証)

【図 10】



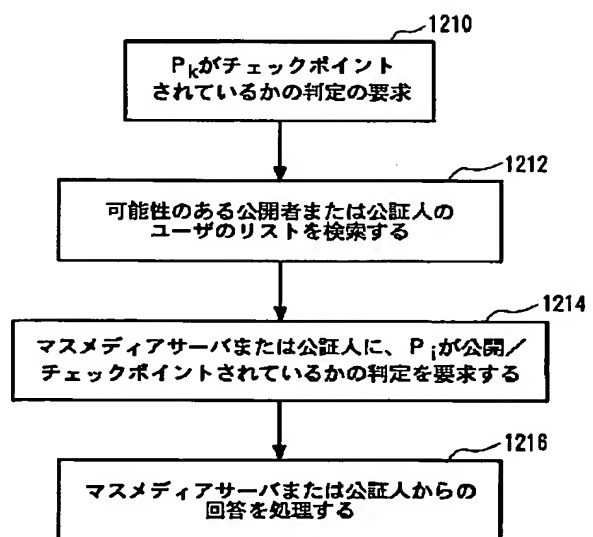
【図 12】

図 12



【図 13】

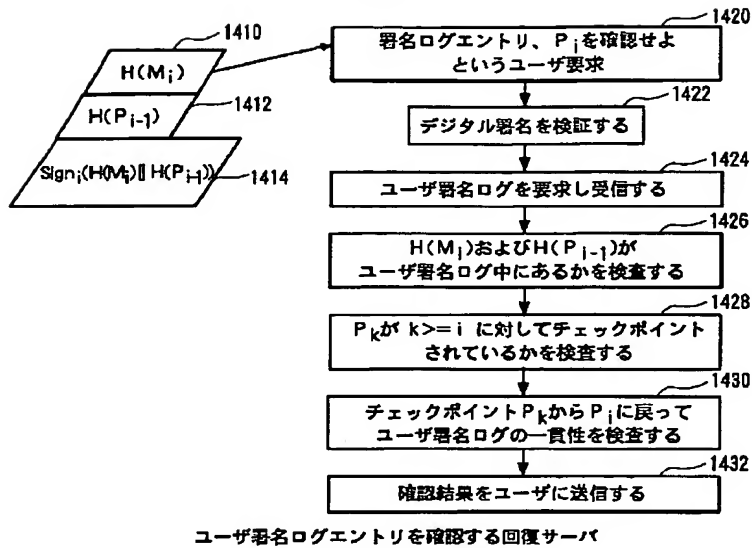
図 13



署名ログエントリがチェックポイント  
されているかを判定する回復サーバ

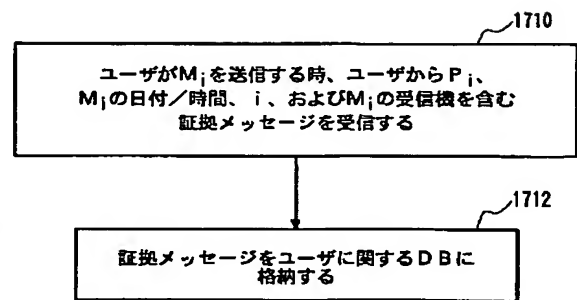
【図 14】

図 14



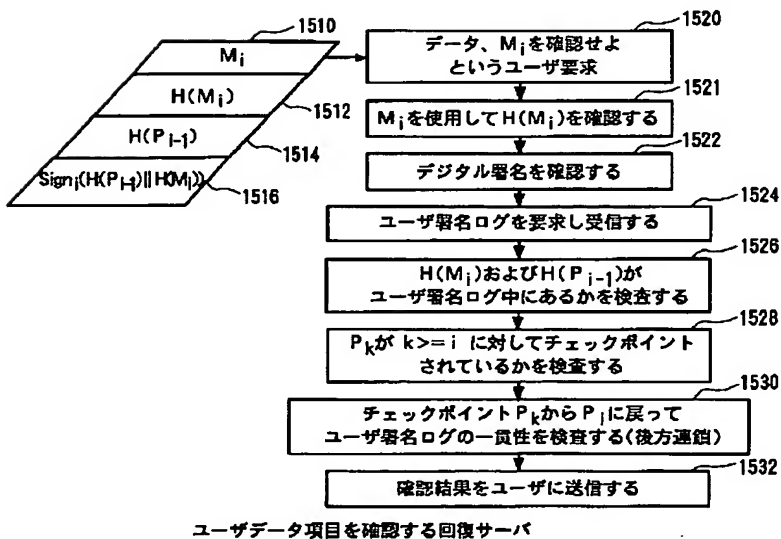
【図 16】

図 16



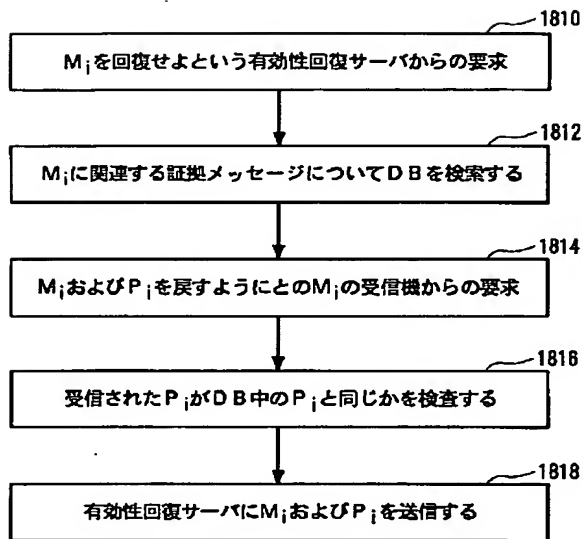
【図 15】

図 15



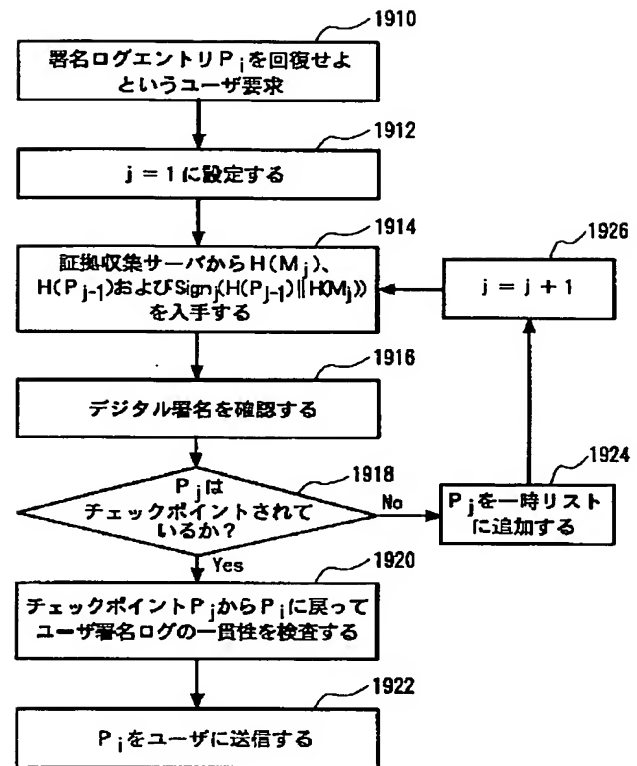
【図 17】

図 17



【図 18】

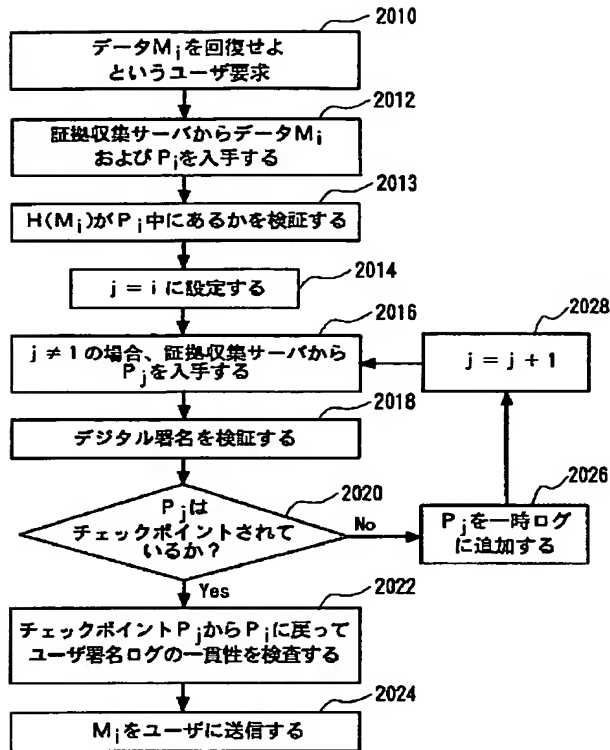
図 18



【図19】

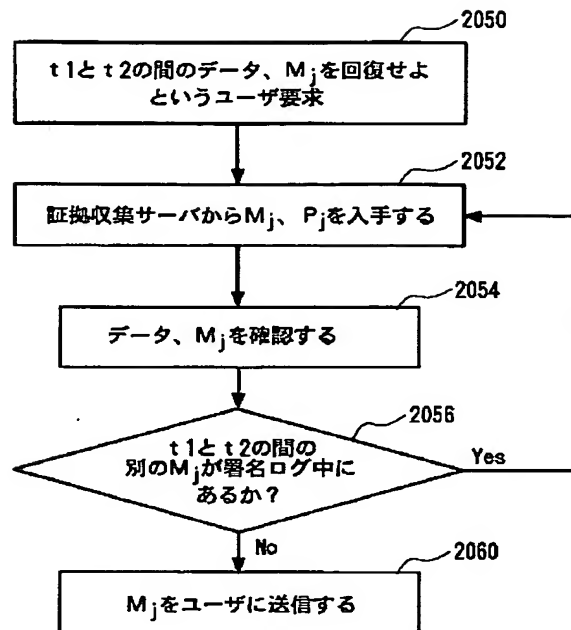
【図20】

図19



ユーザデータ項目を回復する回復サーバ

図20



2つの時点間のユーザデータを回復する回復サーバ

フロントページの続き

(72)発明者 洲崎 誠一  
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 佐々木 良一  
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 宝木 和夫  
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 豊島 久  
 東京都江東区新砂一丁目6番27号 株式会社日立製作所公共システム事業部内

(72)発明者 松木 武  
 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所情報サービス事業部内

Fターム(参考) 5J104 AA09 AA11 AA12 EA19 JA01  
 JA21 LA01 LA03 LA04 LA06  
 MA01 NA02 NA12 NA27

【公報種別】特許法第17条の2の規定による補正の掲載  
【部門区分】第7部門第3区分  
【発行日】平成17年9月2日(2005.9.2)

【公開番号】特開2002-335241(P2002-335241A)  
【公開日】平成14年11月22日(2002.11.22)  
【出願番号】特願2002-59674(P2002-59674)  
【国際特許分類第7版】

H 0 4 L 9/32  
G 0 9 C 1/00

【F I】

H 0 4 L 9/00 6 7 5 B  
G 0 9 C 1/00 6 4 0 D

【手続補正書】

【提出日】平成17年3月7日(2005.3.7)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

ユーザ情報を回復および確認するシステムであって、  
前記ユーザ情報に関連する暗号化情報を含む署名ログを備えるユーザシステムと、  
通信ネットワークを介して前記ユーザシステムと結合され、ユーザ情報を復元する回復システムと、  
前記通信ネットワークを介して前記ユーザシステムと結合され、前記署名ログを使用して復元ユーザ情報を確認する有効性システムとを備えるシステム。

【請求項2】

請求項1記載のシステムであって、  
前記ユーザ情報が前記署名ログのログエントリを含むシステム。

【請求項3】

請求項1記載のシステムであって、  
前記ユーザ情報がユーザメッセージを含むシステム。

【請求項4】

請求項1記載のシステムであって、  
前記暗号化情報がハッシュ値を含むシステム。

【請求項5】

請求項1記載のシステムであって、  
前記署名ログが、前記署名ログの第2のログエントリによって部分的に決定される前記署名ログの第1のログエントリを含むシステム。

【請求項6】

ユーザメッセージが有効かどうかを判定するシステムであって、ログを有するユーザコンピュータシステムと、  
前記ユーザコンピュータシステムと結合され、前記ログを使用して前記ユーザメッセージを確認する確認ユニットとを備え、  
前記ログは、前記ユーザによって送信されるメッセージに関連するログエントリを含み、  
前記ログエントリは、前記ログの前のログエントリに関連する情報を含むデジタル署名

を有するシステム。

【請求項 7】

請求項 6 記載のシステムであって、さらに、

前記ユーザメッセージが失われている時、前記確認ユニットに応答して前記ユーザメッセージを取り出す収集ユニットを備えるシステム。

【請求項 8】

請求項 6 記載のシステムであって、さらに、

前記ユーザメッセージが失われている時、前記確認ユニットに応答して前記メッセージの受信機から前記メッセージのコピーを取り出す収集ユニットを備えるシステム。

【請求項 9】

請求項 6 記載のシステムであって、さらに、

前記ログの選択されたログエントリを公開する公開ユニットを備えるシステム。

【請求項 10】

請求項 9 記載のシステムであって、

前記選択されたログエントリが前記ユーザメッセージを確認する際使用されるシステム

。

【請求項 11】

請求項 9 記載のシステムであって、

公開ユニットが新聞発行者またはウェブサイトからなるグループから選択されるシステム。

【請求項 12】

請求項 6 記載のシステムであって、さらに、

前記ログの選択されたログエントリを登録する公証人ユニットを備えるシステム。

【請求項 13】

請求項 6 記載のシステムであって、さらに、

前記ユーザコンピュータシステムに結合されるログチェーンクロスユニットと、

前記ユーザコンピュータシステムと第 2 のユーザコンピュータシステムの間のトランザクションを記録する前記第 2 のユーザコンピュータシステムとを備えるシステム。

【請求項 14】

請求項 6 記載のシステムであって、さらに、

前記ユーザコンピュータシステムに結合されるログチェーンクロスユニットと、

前記ユーザコンピュータシステムと第 2 のユーザコンピュータシステム間のトランザクションを促進する前記第 2 のユーザコンピュータシステムとを備えるシステム。